REMARKS

This Amendment is in response to the Office Action dated January 14, 2003. Claims 1-30 are pending. Claims 1-30 are rejected. Claims 1, 11 and 21 have been amended. Accordingly, claims 1-30 remain pending in the present application.

Amended Claims

Applicant amended independent claims 1, 11 and 21 to clarify the present invention. Claims 1, 11 and 21 were amended to recite that "the value of the first system is associated with a particular transaction session." Support for this amendment is found in the Specification at page 5, lines 4-22. Thus, no new matter has been presented.

35 U.S.C. §102 Rejections

The Examiner rejected claims 1-5, 11-15 and 21-25 under 35 U.S.C. §102(b) as being anticipated by Kirsch (U.S. Patent No. 5,963,915). In so doing, the Examiner stated:

> **As per claims 1, 11, and 21, Kirsch clearly discloses a method, system, and computer readable medium for conducting a transaction over a network, the network including a first system and a second system, the method, system, and program instructions comprising the steps of:**
> **(a) initiating a transaction;**
> **(b) comparing a value of the first system with a value of the second system; and**
> **(c) continuing the transaction based on the comparison (See Kirsch abstract, figure 3 and associated text, column 3, lines 4-32, column 4, lines 48-64, and column 13, lines 15-51).**

Applicant respectfully traverses.

The present invention is directed to a method and system for conducting a transaction over a network such as the Internet. Through the present invention, a customer purchasing a downloadable file over the Internet will not be charged more than once for a single file(s) if the connection to the Internet is somehow lost while the file(s) is being downloaded. According to

the present invention, when the customer initiates a transaction session via a computer system, e.g., by accessing a web site and selecting a file(s) for download, the server (that supports the web site) determines whether the transaction session is a new session or one that was previously started and interrupted. The server makes this determination by comparing a value of the customer's computer system with a value of its system. The value of the customer's computer system is associated with a particular transaction session. (Spec. at page 4, line 17 to page 5, line 22).

If the value of the customer's computer system does not match the value of the server, the server will generate and store an encryption key. This key is associated with the transaction session and is used to encrypt the requested file(s). A portion of the key is then stored in the customer's system. (Spec. at page 5, lines 5-15). The value of the customer's computer system includes the portion of the key. If, on the other hand, the values match, the transaction session is one that was previously initiated but interrupted, and the server will resume the previously interrupted session. (Spec. at page 5, lines 19-22). Once the encrypted file(s) has been downloaded successfully and the customer has paid the fee, the remaining portion of the key is provided to the customer. (Spec. at page 6, lines 6-9).

The present invention, as recited in claim 1, provides:

> 1. A method for conducting a transaction over a network, the network including a first system and a second system, the method comprising the steps of:
> (a) initiating a transaction session;
> (b) comparing a value of the first system with a value of the second system, wherein the value of the first system is associated with a particular transaction session; and
> (c) continuing the transaction based on the comparison.

Claims 11 and 21 are system and computer product claims having scopes similar to that of claim 1.

Kirsch is directed to a method for efficiently performing secure purchase transactions

between a client and a merchant over the Internet. In Kirsch, "[a] persistent predetermined coded identifier is established on the client browser corresponding to an account record stored by the merchant server." When the client wishes to purchase a product or service, the coded identifier is automatically transmitted to the merchant along with the client's selection, and the merchant "validates the predetermined coded identifier against the server stored account record." (Abstract; col. 4, lines 48-64). According to Kirsch, the predetermined coded identifier includes information sufficient to *authenticate* the client to the merchant and is stored in a cookie on the client system. (Col. 7, lines 60-64). The cookie can also encode "other identifying information . . . to uniquely or at least substantially associate the cookie with a specific combination of the client browser and client system." (Col. 13, lines 15-22). The cookie is used by the merchant "to perform a database look-up to identify a client user account record. . . . The cookie data can then be validated against the information present in the account record. (Col. 13, lines 32-39).

Kirsch fails to teach or suggest "comparing a value of the first system with a value of the second system, wherein the value of the first system is associated *with a particular transaction session*," as recited in claims 1, 11 and 21. In the present invention, the value of the first system includes a portion of an encryption key which was generated by the second system when the particular transaction session was initiated. Accordingly, the value of the first system is associated with the particular transaction session. In contrast, Kirsch compares the information in client system (first system) to the information in the merchant system (second system) in order to *authenticate* the client. The information in the client system (first system) is associated *with the client*, e.g., name, password, credit card number, type of credit card, expiration date, billing address (col. 12, lines 65-67) and other *identifying* information (col. 13, lines 15-22), and *not* associated with the particular transaction session.

This difference is logical because Kirsch addresses a completely different aspect of

electronic commerce than the present invention. In particular, Kirsch is *client*-oriented, i.e. ensuring that a client has an established relationship with the merchant, while the present invention is *transaction*-oriented, i.e., ensuring that a transaction is completed before requiring payment. Accordingly, Kirsch provides no solution to the problem addressed by the present invention.

Because Kirsch fails to teach or suggest "comparing a value of the first system with a value of the second system, wherein the value of the first system is associated with a particular transaction session," as recited in claims 1, 11 and 21, Applicant respectfully submits that claims 1, 11 and 21 are allowable. Claims 2-5, 12-15, and 22-25 depend on claims 1, 11 and 21, and the above arguments apply with equal force. Therefore, Applicant respectfully submits that claims 2-5, 12-15, and 22-25 are also allowable.

35 U.S.C. §103 Rejections

The Examiner rejected claims 6-10, 16-20, and 16-30 under 35 U.S.C. 103(a) as being unpatentable over Kirsch in view of Graunke et al. (U.S. Patent No. 5,991,399). In so doing, the Examiner stated:

> **As per claims 6, 16, and 26, Kirsch discloses all the limitations of claims 5, 15, and 25, further; Graunke clearly teaches,**
> **if the value in the cookie does not match the value in the server system, step (c) further comprises:**
> - **(c1) generating an encryption key;**
> - **(c2) storing a portion of the encryption key in the cookie; and**
> - **(c3) storing the entire encryption key on the server system (See Graunke abstract, figures 2, 4A and 4B and associated text, column 3, lines 5-20 and 60-68, column 6, lines 17-35, column 7, lines 8-68, and column 8, lines 1-31). . . .**
>
> **As per claims 9, 19, and 29, Kirsch discloses all the limitations of claims 5, 15, and 25, further; Graunke clearly teaches, if the value in the cookie does match the value in the server system, ABC discloses that step (c) further comprises:**
> - **(c1) allowing the server system to transfer encrypted information to the client system; and**
> - **(c2) allowing the server system to transfer a remaining portion of the encryption k y to the client system whereby the encryption key is capable of being utilized by the client system t decrypt the encrypted information (see Graunke abstract, figures 2, 4A and 4B and associated text, column 3, lines 5-20 and 60-68, column 6,**

lines 17-35, column 7, lines 8-68, and column 8, lines 1-31).

Applicant respectfully submits that claims 6-10, 16-20, and 16-30 depend on claims 1, 11 and 21, respectively, and the arguments regarding claims 1, 11 and 21 apply with equal force. As such, claims 6-10, 16-20, and 16-30 are allowable over the cited references.

Applicant also submits that claims 6-10, 16-20, and 16-30 are allowable for independent and additional reasons. For ease of reference, claims 6-10 are provided below.

> 6. The method of claim 5 wherein if the value in the cookie does not match the value in the server system, step c) further comprises:
>
> c1) generating an encryption key;
>
> c2) storing a portion of the encryption key in the cookie; and
>
> c3) storing the entire encryption key on the server system.
>
> 7. The method of claim 6 wherein step c) further comprises:
>
> c4) allowing the server system to transfer encrypted information to the client system; and
>
> c5) allowing the server system to transfer a remaining portion of the encryption key to the client system whereby the encryption key is capable of being utilized by the client system to decrypt the encrypted information.
>
> 8. The method of claim 7 wherein step c5) is performed in response to a payment transaction from the client system to the server system.
>
> 9. The method of claim 5 wherein if the value in the cookie does match the value in the server system, step c) further comprises:
>
> c1) allowing the server system to transfer encrypted information to the client system; and
>
> c2) allowing the server system to transfer a remaining portion of the encryption key to the client system whereby the encryption key is capable of being utilized by the client system to decrypt the encrypted information.
>
> 10. The method of claim 9 wherein step c2) is performed in response to a payment transaction from the client system to the server system.

Claims 16-20 and 26-30 are system and computer product claims having scopes similar to claims 6-10.

Graunke is directed to the "[s]ecure distribution of a private key to a user's application program (also called a 'trusted player' such as a DVD player or CD-ROM player) with conditional access based on verification of the trusted player's integrity and authenticity."

(Abstract). Graunke discloses "generating an asymmetric key pair . . . , encrypting predetermined data with the generated public key, building an executable tamper resistant key module identified for the program, the executable tamper resistant key module including the generated private key and the encrypted predetermined data, and sending the executable tamper resistant key module to the remote system. The tamper resistant key module is then executed on the remote system to check the integrity and authenticity of the program and the integrity of the tamper resistant key module itself. If the validation process is successful, then the encrypted predetermined data is decrypted with the generated private key included in the tamper resistant key module." (Col. 3, lines 5-20).

Kirsch in combination with Graunke discloses a system whereby a client wishing to purchase digital content from a provider is authenticated via Kirsch's cookie and encryption keys for decrypting the digital content are securely transmitted to the client via Graunke's key module. Applicant respectfully submits that this combination fails to teach or suggest the present invention, as recited in claims 6-10, 16-20, and 26-30.

With regard to claims 6, 16 and 26, Kirsch in view of Graunke fails to teach or suggest "generating an encryption key," and "storing *a portion* of the encryption key in the cookie" "*if* the value in the cookie *does not* match the value in the server system," as recited in claims 6, 16 and 26. In the present invention, if the value in the cookie *does not* match the value in the server system, i.e., a new transaction has been initiated, an encryption key is generated and a portion of the key is stored in the cookie. Thus, generating an encryption key is conditioned upon whether the values match. If the values *do* match, an encryption key *will not* be generated.

In contrast to the present invention, Graunke generates the key pair for encrypting the predetermined data when the data is *created.* (Col. 8, lines 2-5; Figure 4A (step 102)). In addition, Graunke generates the key module when the program on the remote site requests the

keys for decrypting the encrypted data. (Col. 7, lines 16-30; Col. 8, lines 13-20; Figure 4A (step 106)). In both instances, the generation of an encryption key or key module is *not* conditioned upon whether values in a cookie *match* those in the server system. Accordingly, Graunke fails to teach or suggest "generating an encryption key" "*if* the value in the cookie *does not* match the value in the server system," as recited in claims 6, 16 and 26.

Moreover, nothing in Kirsch in view of Graunke teaches or suggests "storing *a portion* of the encryption key in the cookie," as recited in claims 6, 16 and 26. According to Graunke, the key pair for decrypting the encrypted data is stored in the server database (col. 8, lines 2-5), and is also included in the key module (col. 7, lines 53-55). The key module also includes "an asymmetric public key for verifying the digital signature of the manifest . . . . and an asymmetric private key for decrypting the encrypted symmetric public keys when the validity of the trusted player on the client is assured." (Col. 7, lines 46-57). The key module *does not* include *a portion* of a key. Nothing in Kirsch in view of Graunke teaches or suggests "storing a *portion* of the encryption key in the cookie," as recited in claims 6, 16 and 26.

Because Kirsch in view of Graunke fails to teach or suggest "generating an encryption key," and "storing *a portion* of the encryption key in the cookie" "*if* the value in the cookie *does not* match the value in the server system," as recited in claims 6, 16 and 26, claims 6, 16 and 26 are allowable.

As for claims 7, 9, 17, 19, 27 and 29, Applicant respectfully submits that Kirsch in view of Graunke fails to teach or suggest "allowing the server system to transfer *a remaining portion* of the encryption key to the client system." As stated above, Graunke's key module *does not* include *a portion* of an encryption key. All of the keys in the key module are complete public or private keys. Accordingly, Applicant respectfully submits that claims 7, 9, 17, 19, 27 and 29 are allowable over the cited references.

Claims 8, 10, 18, 20, 28 and 30 depend on claims 7, 9, 17, 19, 27 and 29, respectively, and therefore the above arguments apply with equal force. Thus, claims 7, 9, 17, 19, 27 and 29 are also allowable over the cited references.

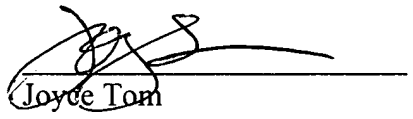
Conclusion

In view of the foregoing, Applicant submits that claims 1-30, as now presented, are patentable over the cited references. Applicant, therefore, respectfully requests reconsideration and allowance of the claims as now presented.

Applicant's attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,

May 12, 2003
Date



Joyce Tom
Attorney for Applicants
Sawyer Law Group LLP
Reg. No.48,681
(650) 493-4540